东方电气 DONGFANG ELECTRIC

电站控制系统网络安全攻击研究

中国东方电气集团中央研究院　袁晓舒

东方电气
DONGFANG ELECTRIC

1	中国东方电气集团简介
2	拒绝服务攻击对电站控制系统危害
3	现场总线攻击对电站控制系统危害
4	总结

DEC 东方电气 DONGFANG ELECTRIC

中国东方电气集团有限公司

中国东方电气集团有限公司（简称“东方电气”）是党中央、国务院确定的“涉及国家安全和国民经济命脉的国有重要骨干企业”之一，中国最大的发电设备制造、电站工程承包及机电成套设备出口基地之一，属国务院国资委监管国有独资企业。

- 水电　单机最大1000MW等级系列水轮发电机组
- 火电　单机最大1200MW等级系列火电机组
- 核电　单机最大1700MW等级第三代核电机组主设备
- 燃气发电　E/F级重型燃气轮机
- 风电　单机最大5.5MW等级系列风电机组
- 太阳能发电　100MW级太阳能光热电站、光伏发电站
- 环保　烟气污染物处理、余热锅炉、高效电机等
- 海水淡化　单体最大每日12500吨级海水淡化设备
- 电力电子　大功率变频器、发电装备控制系统、电站DCS控制系统等电力电子产品

火电

DCS、锅炉控制、汽机控制、发电机控制、水处理控制系统、煤处理控制、灰浆处理控制、脱硝处理控制等。

水电

DCS、水轮机控制系统、发电机控制系统、水电厂自动化系统、发电机静态变频启动系统（SFC）等。

风电

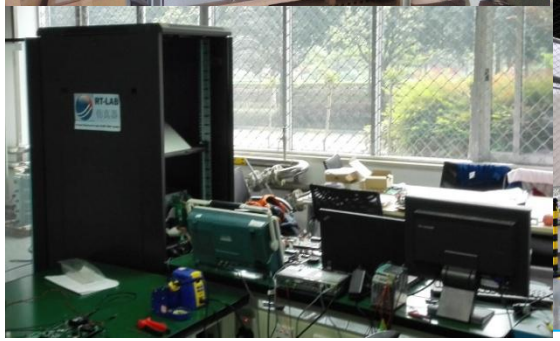
电场SCADA、风机主控系统、变桨控制系统、偏航控制系统、风电变流器、风机振动分析系统、风机消防系统、风机视频监控系统。

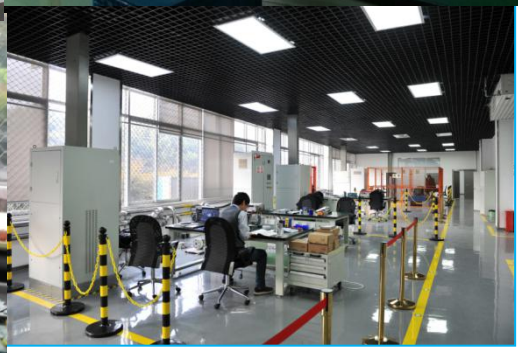
中国东方电气集团有限公司中央研究院

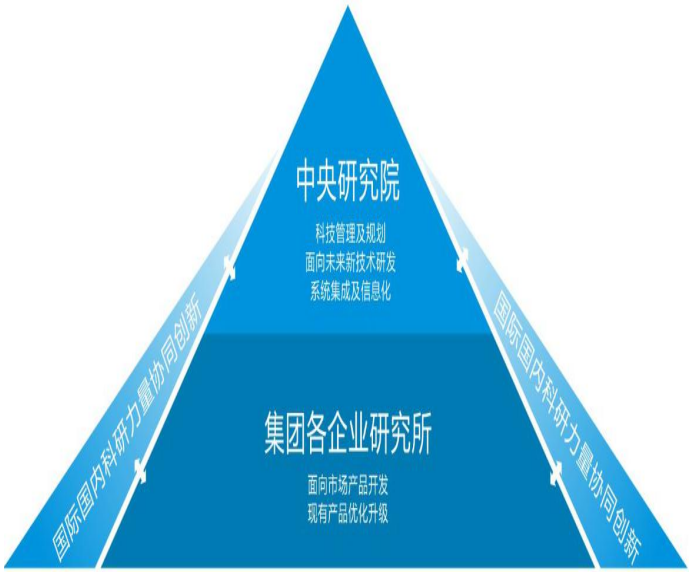
■面向未来：智能装备及制造、电力电子、超导技术、新能源汽车动力总成、先进能源转换技 术、清洁燃烧技术、储能技术、太阳能发电技术、新能源系统集成技术；

■面向企业：共性技术研究、核心技术攻关、智能制造、信息化建设；

■面向工程：电站工程设计、新能源系统设计研究、EPC工程支持及咨询、环保工程设计咨询。



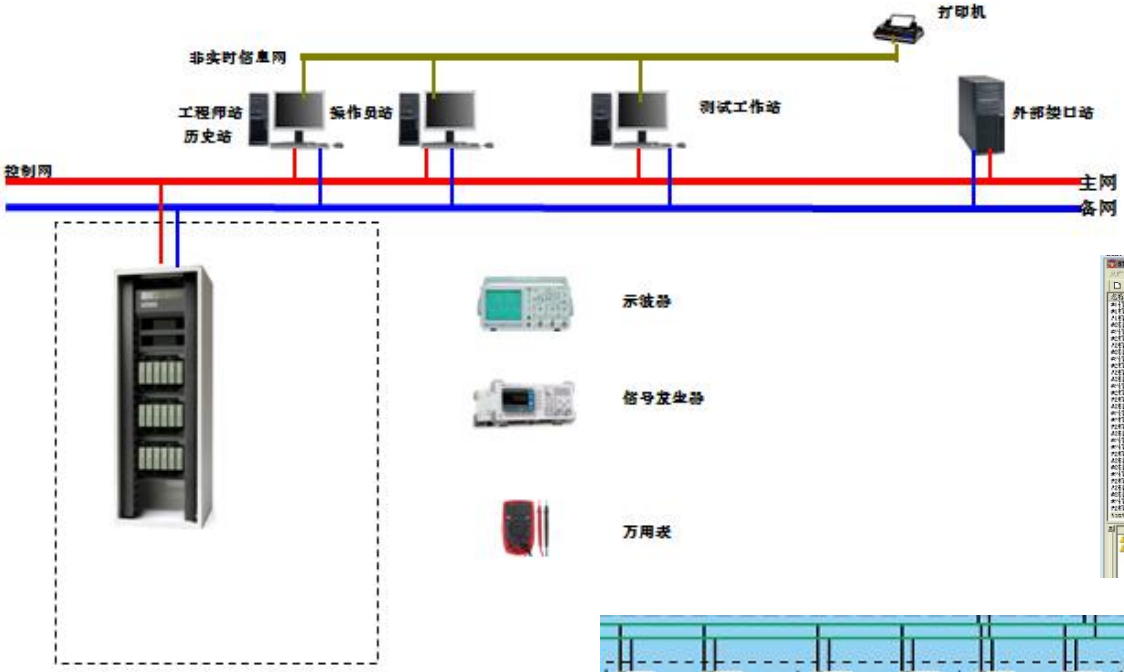


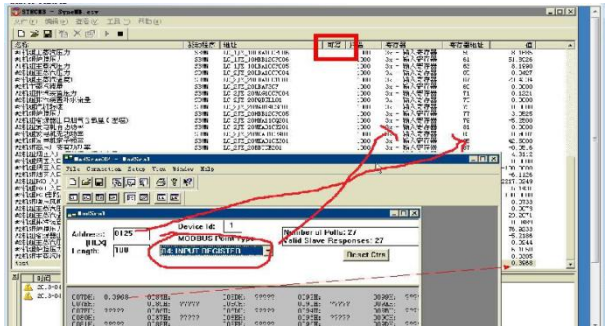


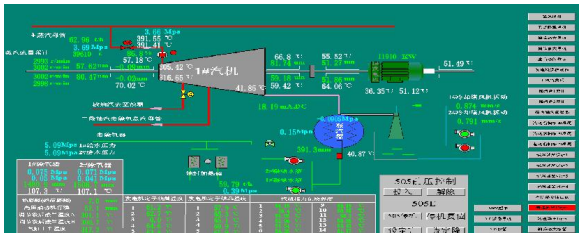
东方电气 DONGFANG ELECTRIC

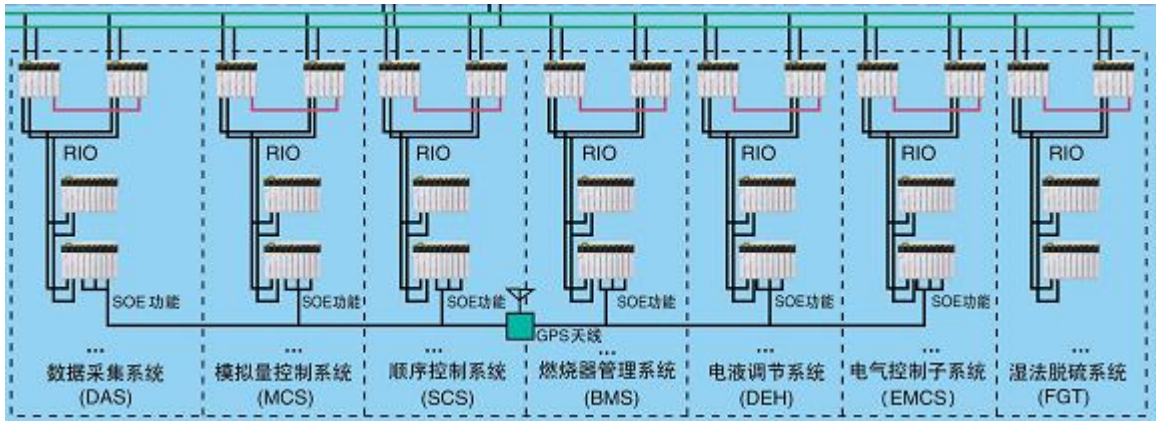
1	中国东方电气集团简介
2	拒绝服务攻击对电站控制系统危害
3	现场总线攻击对电站控制系统危害
4	总结

背景介绍

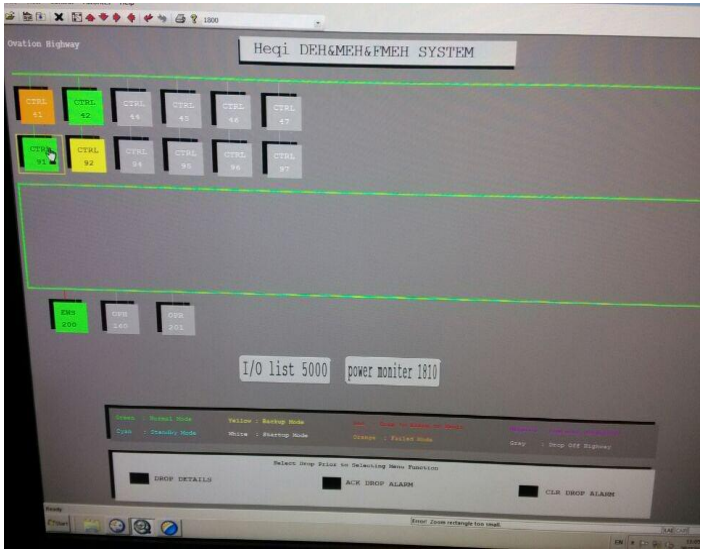

打印机
非实时信息网
工程师站
历史站
操作员站
测试工作站
外部接口站
控制网
主网
备网
示波器
信号发生器
万用表

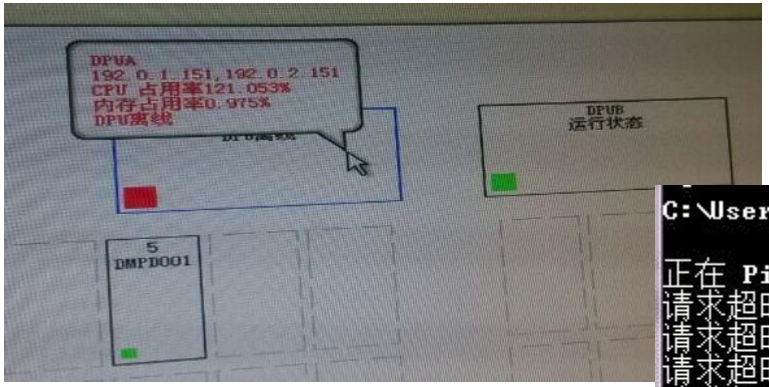





RIO
SOE 功能
SOE功能
GPS天线
数据采集系统
(DAS)
模拟量控制系统
(MCS)
顺序控制系统
(SCS)
燃烧器管理系统
(BMS)
电液调节系统
(DEH)
电气控制子系统
(EMCS)
湿法脱硫系统
(FGT)

SYSFLOOD/UDPFLOOD攻击



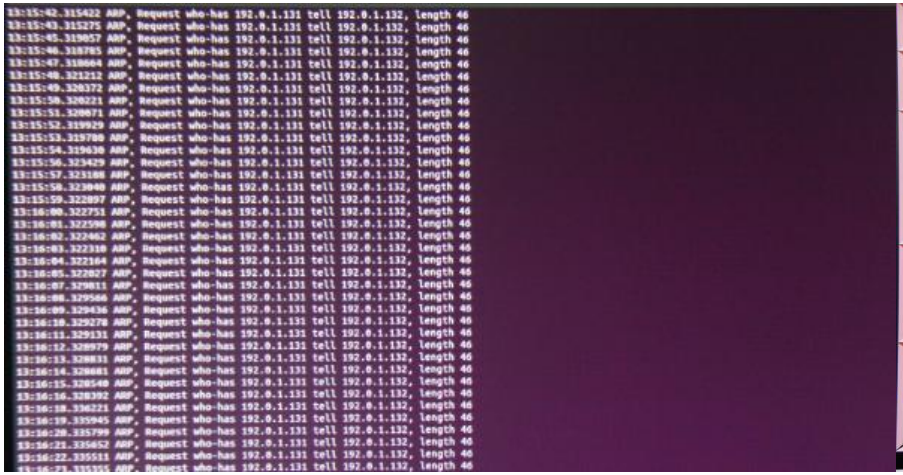


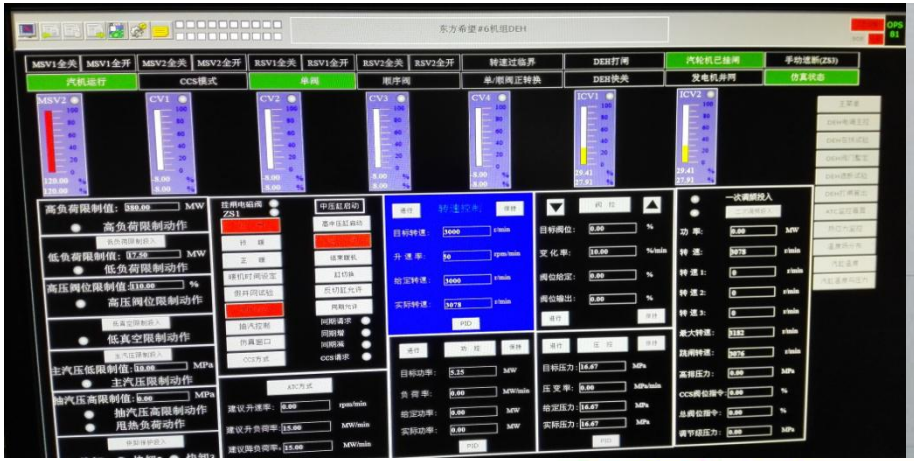

```
C:\Users\Administrator>ping 192.168.2.41

正在 Ping 192.168.2.41 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

192.168.2.41 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),
```

SYSFLOOD/UDPFLOOD攻击

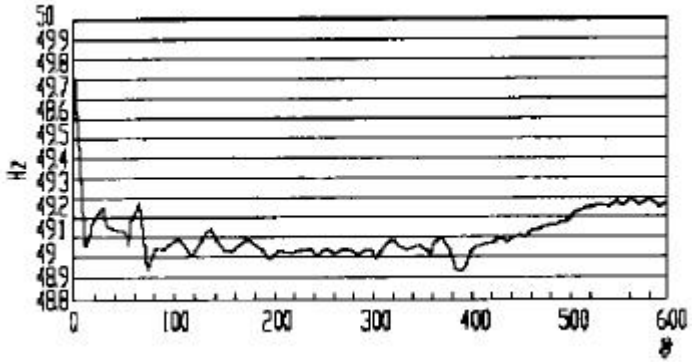


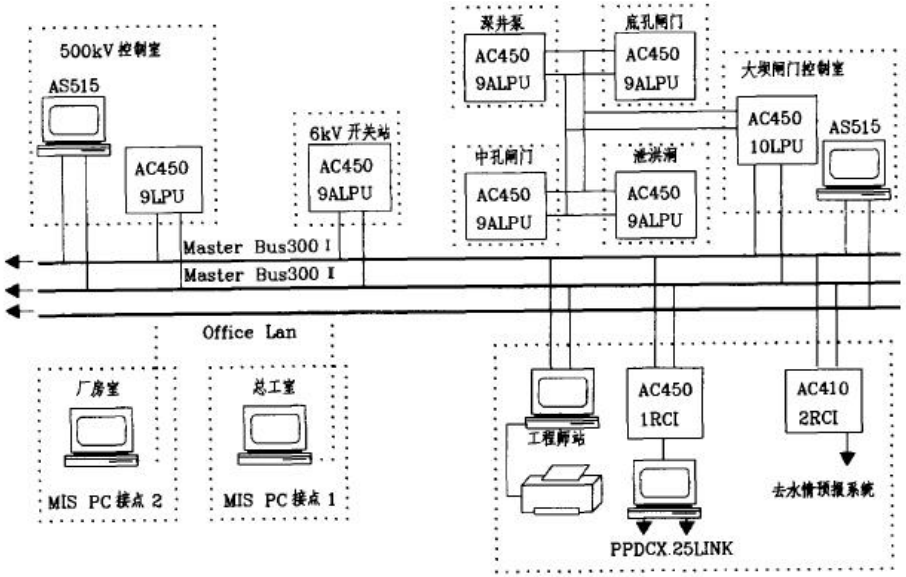


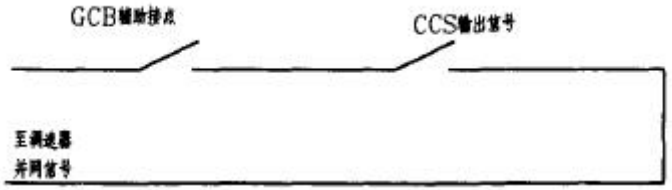
DCS系统信息安全防护

二滩电站事故

- 2000年10月13日，四川二滩水电厂监控系统因异常地接收到外来信号，7秒钟甩出力89万千瓦，导致川渝电网几乎瓦解。

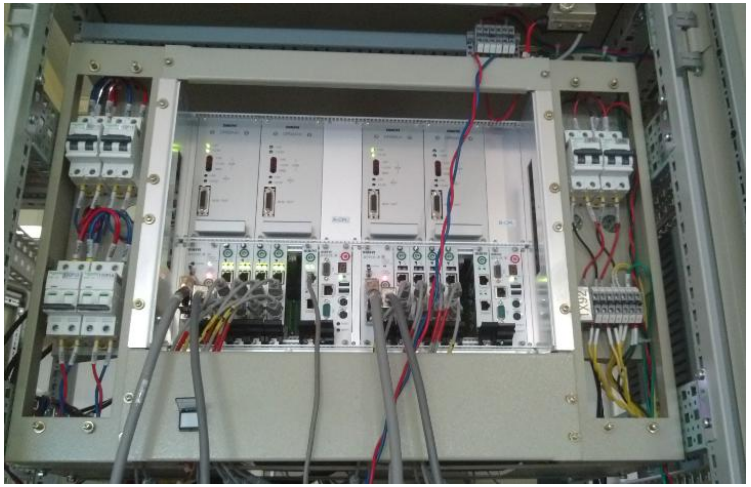


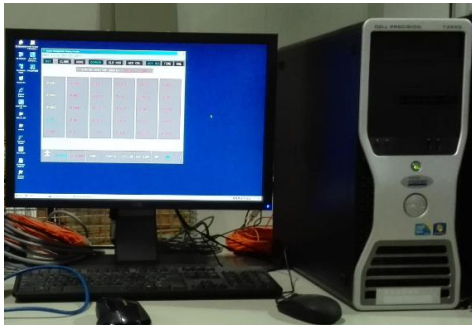




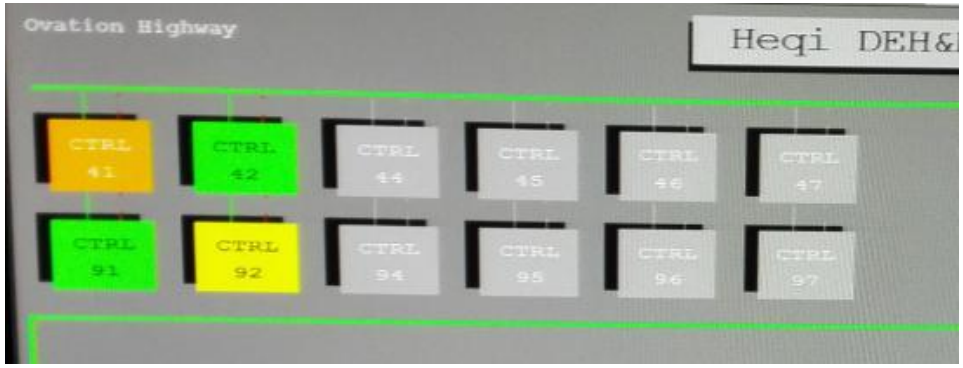
东方电气 DONGFANG ELECTRIC

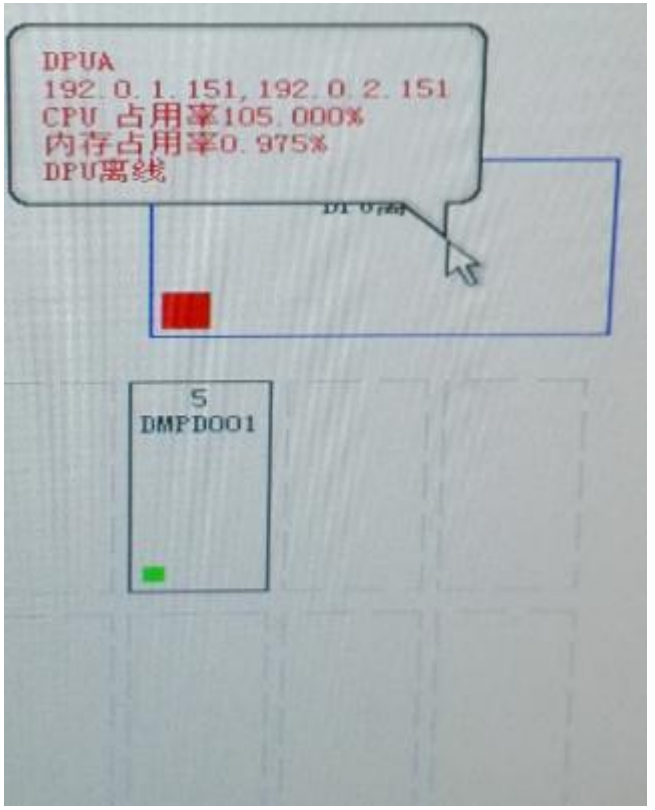
背景介绍

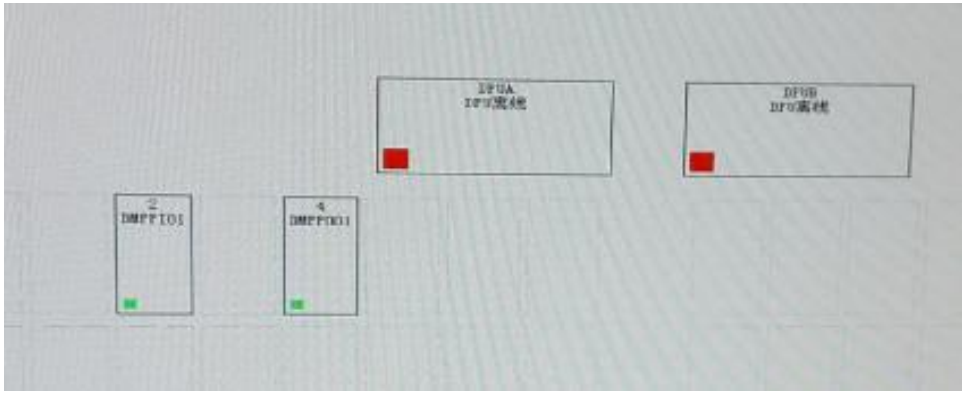




MODBUSTCP攻击

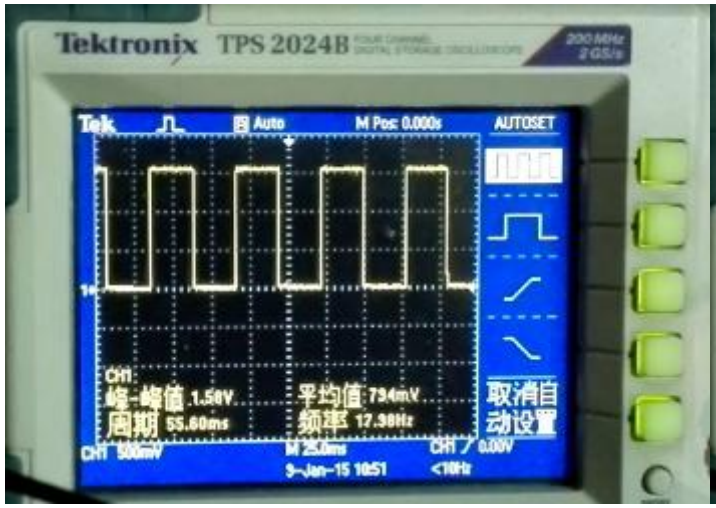


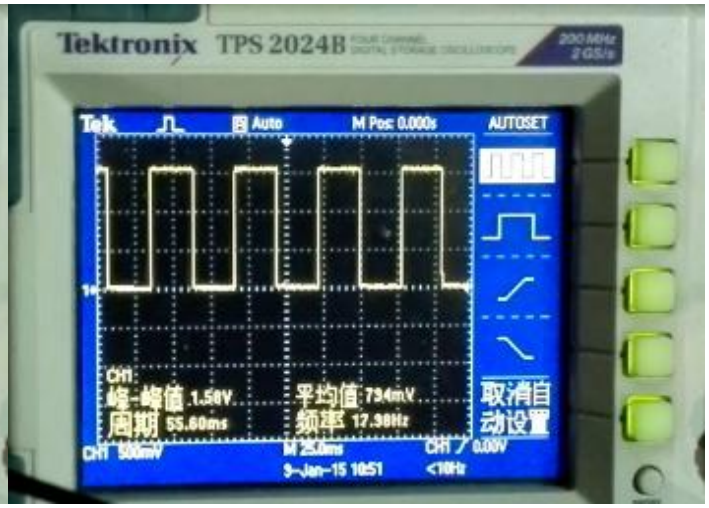




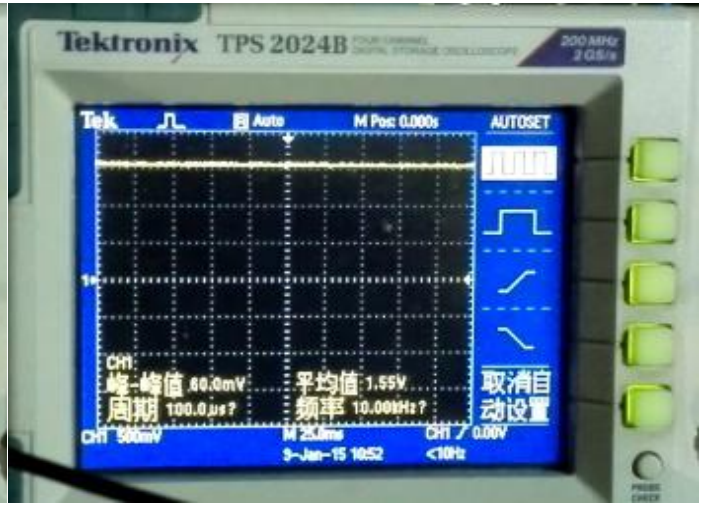

```
-> 0x83d7cc (tHear04): recv fail. rc =0
0x916408 (tDebug): SuspendTasksForReload
0x916408 (tDebug): ResumeTasksForReload
```

MODBUSTCP攻击



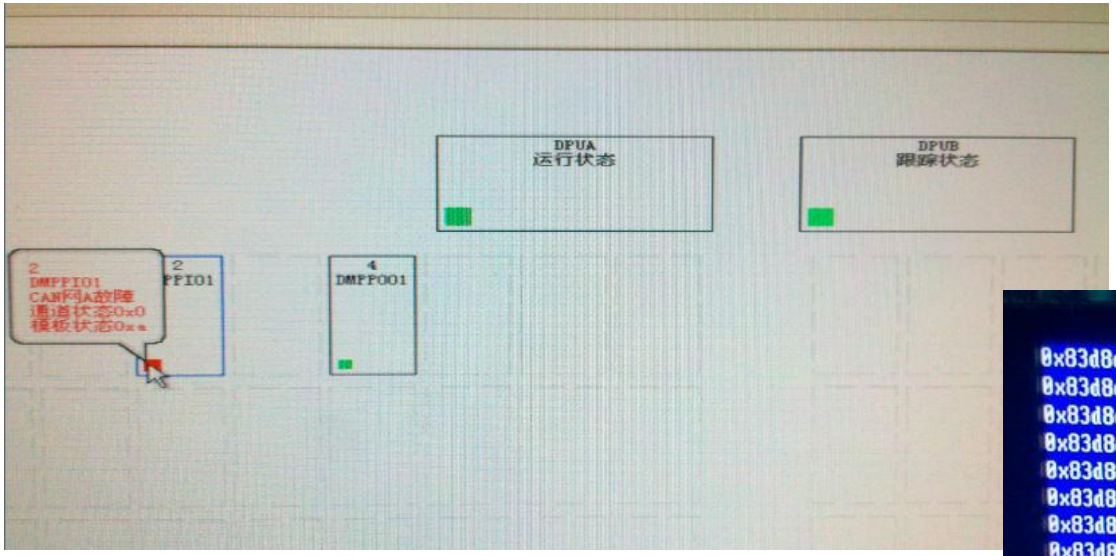


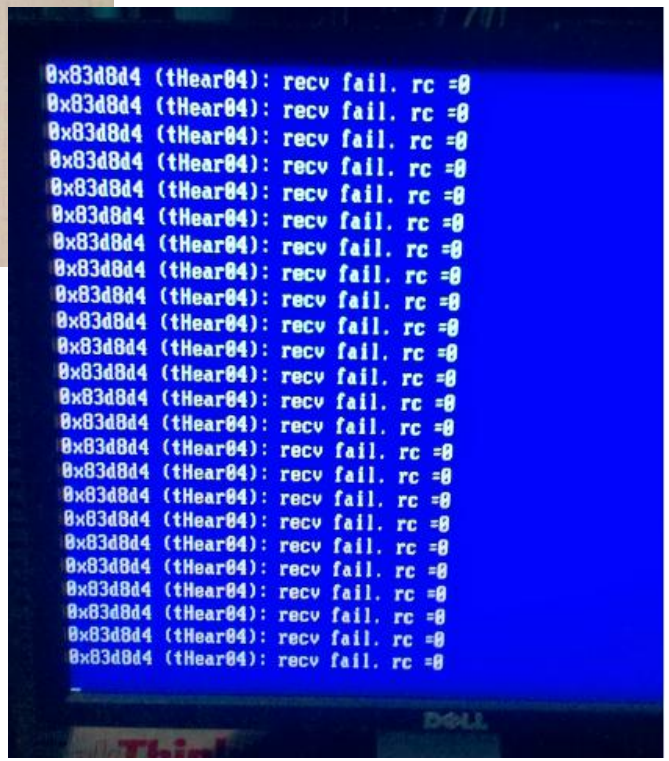
MODBUSTCP攻击



东方电气 DONGFANG ELECTRIC

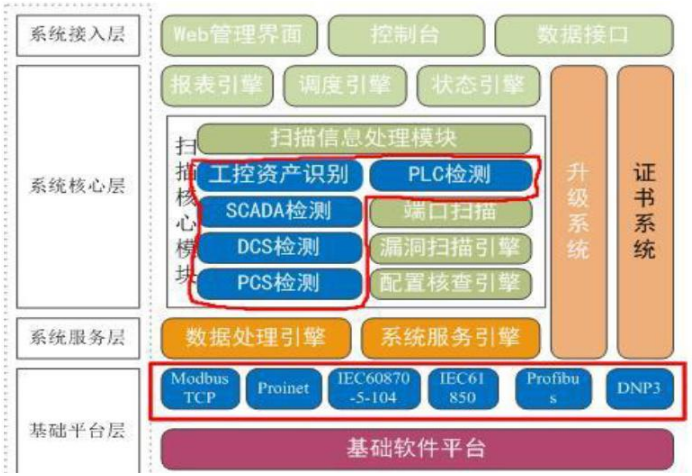
MODBUSTCP攻击

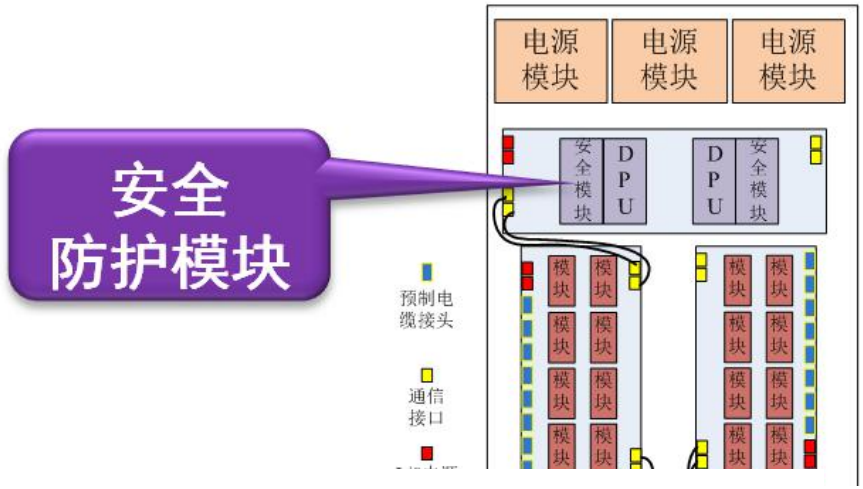


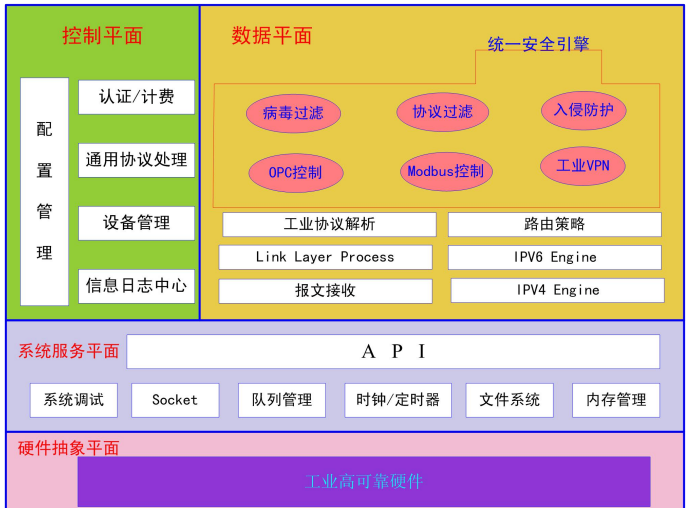


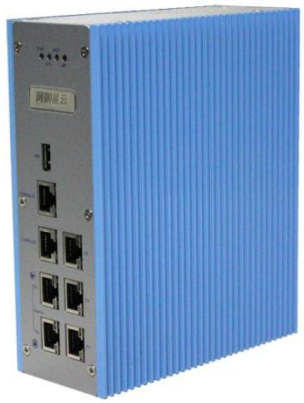
东方电气 DONGFANG ELECTRIC

东方电气 DONGFANG ELECTRIC









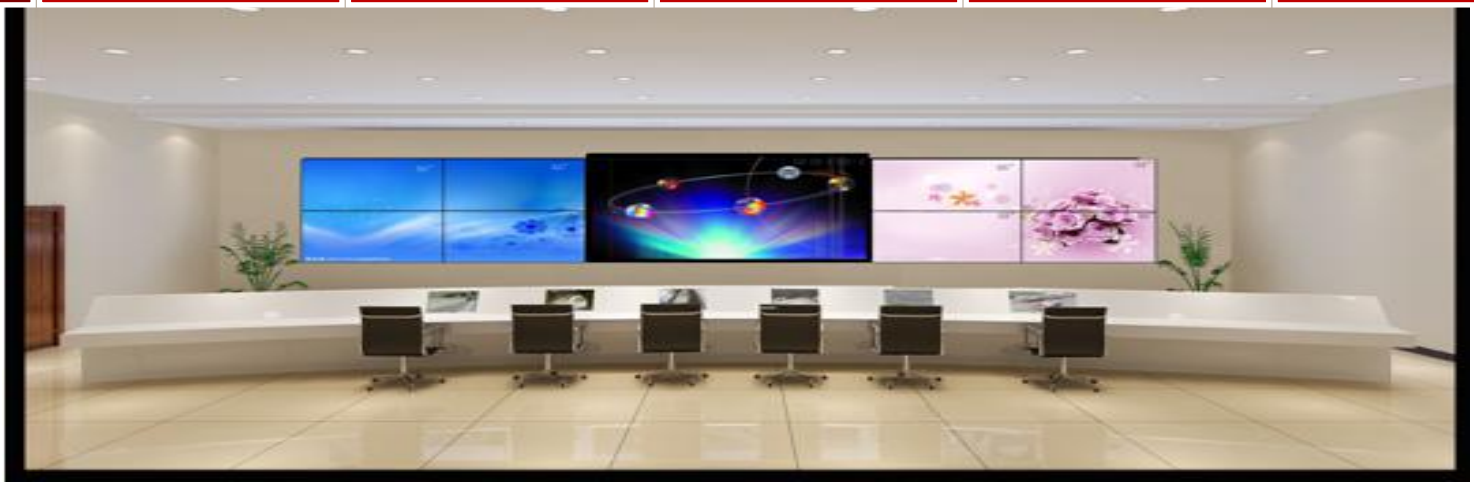
东方电气
DONGFANG ELECTRIC

远程监测

大数据

监测诊断系统平台

- 异常诊断
- 仿真电厂
- 知识库
- 专家库
- 诊断模块
- 诊断报告



以信息安全提升产品价值。

谢谢